## REMARKS

Claims 1-22 are currently pending in the subject application, and are presently under consideration. Claims 1-22 are rejected. Claims 1 and 12 have been amended. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

### I. Objection to Drawings

The drawings have been objected to as failing to comply with 37 CFR 1.84(g) because the margins in FIG. 1 are outside specification, with 37 CFR 1.84(l) because the lines, numbers, and letters in FIGS. 1-3 are not uniformly thick and well-defined, and with 37 CFR 1.84(p)(1) because some of the reference characters in FIGS. 1-3 are not plain and/or legible. A revised drawing set has been attached to this Office Action Response which corrects the aforementioned defects objected to by the Office Action. Accordingly, withdrawal of this objection is respectfully requested.

The drawings have also been objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference characters not mentioned in the description: FIG. 1, items 142, 149, 154; FIG. 2, items 260, 270, 280. Item 149 on FIG. 1 has been omitted from the revised drawing set as it is not necessary to adequately explain the present invention. Item 154 on FIG. 1 has been added to the specification in the above amended paragraph beginning on page 9, line 26. Item 260 on FIG. 2 has been changed to 106 on the revised drawing set to correct the numbering error. It is respectfully submitted that item 142 on FIG. 1 and items 270 and 280 on FIG. 2 do appear in the description (see page 13, line 13 and page 14, lines 12-14, respectively). Accordingly, withdrawal of this objection is respectfully requested.

### II. Rejection of Claims 1-22 Under 35 U.S.C. §112

Claims 1-22 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to point out and distinctly claim the subject matter of the invention. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 1 and 12 have been amended to recite the predetermined pedigree certificate having a level of trust commensurate with a category of hardware of which the provided piece of hardware is a member. This amendment was performed to change the phrase "bearing a relationship to" to "commensurate with" to provide a standard for ascertaining the requisite degree and to allow one with ordinary skill in the pertinent art to be reasonably apprised of the scope of the invention. Accordingly, withdrawal of this rejection is respectfully requested.

## II. Rejection of Claims 1-22 Under 35 U.S.C. §102(e)

Claims 1-22 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,609,198 to Wood, et al. ("Wood"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Amended claims 1 and 12 recite a method and an apparatus, respectively, for automatically tracking a certificate pedigree that comprises a piece of hardware containing a predetermined pedigree certificate stored therein, the predetermined pedigree certificate having a level of trust commensurate with a category of hardware of which the provided piece of hardware is a member. Wood teaches a security architecture in which a single sign-on is provided for multiple information resources, wherein trust level requirements are associated with information resources. The Office Action asserts that the credential disclosed by Wood contains a certificate that is associated with a trust level used for registration, and that this teaches the elements of claim 1 (Office Action dated July 21, 2004, page 6). Representative for Applicant respectfully disagrees.

The pedigree of a certificate is based on the type of storage media on which a certificate was generated and that a corresponding private key is stored (Specification, page 6, ll. 5-12). The significance of a pedigree of a certificate is evident in that a certificate generated on a client PC will typically be less trustworthy than a certificate generated on a hardware token in that hardware tokens are typically more difficult for hackers to compromise than conventional PCs, and hence certificates generated by such tokens have a higher level of trust (Specification, page 6, ll. 18-23). It is the trustworthiness of the certificate generation on a hardware token to prevent

hacking that forms the basis for the pedigree certificate to have a level of trust commensurate with a category of devices with which the piece of hardware is a member, as recited in claims 1 and 12.

Wood teaches that login credentials, which may be hardware, may be obtained and authenticated to a particular trust level (col. 6, ll. 33-34). However, Wood is completely silent as to the use of a pedigree certificate associated with any of the authentication or security credentials disclosed therein. Additionally, the trust level of authentication as taught in Wood corresponds to a trust level requirement of an application or information resource to be accessed (col. 6, ll. 15-17), and is not a level of trust associated with a piece of hardware from which a certificate is generated and on which a private key is stored. Therefore, Wood does not teach a method or apparatus of automatically tracking a certificate pedigree, and further does not teach a piece of hardware containing a predetermined pedigree certificate stored therein, the predetermined pedigree certificate having a level of trust commensurate with a category of devices of which the provided piece of hardware is a member, as recited in claims 1 and 12.

Claims 1 and 12 further recite that an automated registration arrangement provides a new user with an individual signature certificate having a level of trust commensurate with that of the pedigree certificate. The Office Action asserts that this is taught by a session token issued to the user that is commensurate with presented credentials, specifically equating the session token with the individual signature certificate (Office Action dated July 21, 2004; citing Wood, col. 3, ll. 42-53). Representative for Applicant respectfully disagrees.

A signature certificate, as known in the art of Public Key Infrastructure (PKI), is a mechanism for reliably conveying the identity of a key pair's owner to the end user (Specification, page 2, ll. 8-9). The PKI establishes that the user owns a key pair by using the digital certificate, which contains information identifying the owner of the key pair, the public key, and the period of time of validity (Specification, page 2, ll. 16-21). The signature certificate is thus not used to authenticate a user to a given security level.

Wood teaches the authentication of an entity to a first authentication level and associating a unique session identifier with the entity (col. 3, ll. 46-48). The entity would thereafter be

allowed access to a second authentication level using the unique session identifier (col. 3, ll. 51-53). The unique session identifier, as taught by Wood, is therefore merely a password or authentication scheme, and is not a signature certificate. Accordingly, Wood does not teach an automated registration arrangement that provides a new user with an individual signature certificate having a level of trust commensurate with that of the pedigree certificate, as recited in claims 1 and 12.

For the reasons stated above, Wood does not anticipate claims 1 and 12. Accordingly, withdrawal of the rejection of claims 1 and 12, as well as claims 2-11 and 13-22 which depend therefrom, respectively, is respectfully requested.

Claims 3 and 14 recite that one of at least two pieces of information is provided to the user by the automated registration arrangement in response to the user providing an additional piece of information to the automated registration arrangement. Wood teaches that further authentication can be performed by using information encoded within a certificate to query a certificate authority for current status or lookup to an authentication database, and that the configuration could force an additional name/password pair as part of the certificate authentication chain (col. 12, ll. 27-35). Thus, Wood teaches that further information may be needed from the user in response to information entered into the certification authority. However, Wood does not teach that information is provided to the user from the certification authority in response to information entered into the certification authority. Therefore, Wood does not teach that one of at least two pieces of information is provided to the user by the automated registration arrangement in response to the user providing an additional piece of information to the automated registration arrangement, as recited in claims 3 and 14. Withdrawal of the rejection of claims 3 and 14, as well as claims 5, 7, and 9, and 16, 18, and 20, respectively, which depend therefrom, is respectfully requested.

For the reasons described above, claims 1-22 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

## CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Date 10/01/04

Respectfully submitted,

Christopher P. Harris

Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.

526 SUPERIOR AVENUE, SUITE 1111

CLEVELAND, OHIO 44114-1400

Phone: (216) 621-2234

Fax: (216) 621-4072

## DRAWINGS

As required by the Office Action, please substitute the originally submitted drawing sheets with the attached corrected drawing sheets.